# Integral Euler systems and Main Conjectures (Algebraic Number Theory and Related Topics 2015)

AUTHOR(S):

SPRUNG, Florian E. Ito

CITATION:

SPRUNG, Florian E. Ito. Integral Euler systems and Main Conjectures (Algebraic Number Theory and Related Topics 2015). 数理解析研究所講究録別冊 2018, B72: 135-145

ISSUE DATE:

2018-12

URL:

http://hdl.handle.net/2433/244740

*RIMS Kôkyûroku Bessatsu*
**B72** (2018), 135–145

# Integral Euler systems and Main Conjectures

By

Florian E. Ito Sprung*

**Abstract**

We give a strategy for proving the Iwasawa Main Conjecture for weight two modular forms at primes of slope $> 0$.

## § 1. Introduction

Iwasawa theory is a connection between analytic and algebraic objects. When one wants to shed light on an object defined over a base number field $K$, Iwasawa theory provides a way of viewing it as a member of a family of objects over $K_n$, where $K_n$ is an extension of $K$ in a tower of number fields, constructed so that $\mathrm{Gal}(K_n/K) \cong \mathbb{Z}/p^n\mathbb{Z}$ and $\varprojlim_n \mathrm{Gal}(K_n/K) \cong \mathbb{Z}_p$. In the context of an elliptic curve $E$ defined over $\mathbb{Q}$ and in which the base field is also $K = \mathbb{Q}$, we are interested in the following conjecture:

*Conjecture* 1.1 (Birch and Swinnerton-Dyer Conjecture).
I. We have $\mathrm{ord}_{s=1} L(E, s) = r$.
II. For the leading Taylor coefficient in the power series expansion about $s = 1$, we have

$$\frac{L^{(r)}(E, 1)}{r!\Omega} = \#Ш(E/\mathbb{Q}) \cdot \frac{\mathrm{Reg}(E/\mathbb{Q}) \prod_l c_l}{\#E(\mathbb{Q})^2_{\mathrm{tor}}}.$$

Here, $L(E, s)$ is the Hasse-Weil $L$-function of $E$, $\mathrm{ord}_{s=1}$ denotes the order of vanishing at $s = 1$, $L^{(r)}$ is the $r$-th derivative, and $\Omega$ the real period. On the algebraic side, $r$ denotes the Mordell–Weil rank of $E(\mathbb{Q})$, and $\mathrm{Reg}(E/\mathbb{Q}), E(\mathbb{Q})_{\mathrm{tor}}$, and $c_l$ denote the regulator, torsion subgroup, and Tamagawa factor at $l$ respectively. The most important term is the Šafarevič–Tate group $Ш(E/\mathbb{Q})$, whose order is not known to be finite.

Received April 20, 2016. Revised December 28, 2016.
2010 Mathematics Subject Classification(s): Primary: 11G40, 11F67. Secondary: 11R23, 11G05.
*Key Words*: *Iwasawa Theory.*
*Princeton University and the Institute for Advanced Study
e-mail: fsprung@princeton.edu

The merit of Iwasawa Theory is that it equips us with a strategy for proving (II) prime by prime when part (I) is known. For part (I), the current status is that under mild assumptions, we have for $m \in \{0, 1\}$ that

$$\text{“}\operatorname{ord}_{s=1} L(E, s) = m\text{” if and only if “}r = m \text{ and } Ш(E/\mathbb{Q}) \text{ is finite”}$$

via works of Coates–Wiles, Kolyvagin, Gross–Zagier, Rubin, Kato, Skinner–Urban, and Skinner–Zhang.

One consequence of the Iwasawa main conjecture is the $p$-primary part of (II) in the above conjecture, i.e. the equality:

$$\left|\frac{L(E,1)}{\Omega}\right|_p = \left|\#Ш(E/\mathbb{Q}) \prod_l c_l\right|_p$$

in the rank 0 case, and

$$\left|\frac{L'(E,1)}{\Omega \operatorname{Reg}(E/\mathbb{Q})}\right|_p = \left|\frac{\#Ш(E/\mathbb{Q}) \prod_l c_l}{\#E(\mathbb{Q})^2_{\mathrm{tor}}}\right|_p$$

in the rank 1 case.

As for the status of the main conjecture, it is known when $p$ is of good reduction, and $E$ has complex multiplication. In fact, Rubin [Ru91] proved this for ordinary primes, i.e. those primes for which $p$ is coprime to $a_p = p+1-\#E(\mathbb{F}_p)$, and in the supersingular case ($p|a_p$), it was proved by Pollack and Rubin [PR04]. For the non-CM case, Kato constructed an Euler system to prove one inclusion. The reverse inclusion was proved by Skinner and Urban in the ordinary case. These theorems come with small assumptions. Recently, Wan in [W] has posted a proof of the main conjecture for elliptic curves in the case $a_p = 0$, a subcase of the supersingular case. For elliptic curves, we note that $a_p = 0$ and $p$ supersingular are equivalent as long as $p \geqslant 5$. The purpose of this paper is to sketch a strategy that works for the general supersingular case, in which $p$ is odd, cf. [S].

## § 2. Main Conjectures in the weight two case

We describe the form of the main conjecture in the case of ordinary reduction, before moving on to the formulation in the supersingular case.

### § 2.1. The classical form of a Main Conjecture

Classically, a main conjecture has the following form: Let $M$ be a compact $\mathbb{Z}_p$-module with a continuous action of the Galois group $\operatorname{Gal}(\mathbb{Q}_\infty/\mathbb{Q})$, where $\mathbb{Q}_\infty$ denotes

the cyclotomic $\mathbb{Z}_p$-extension of $\mathbb{Q}$. We can regard $M$ as a $\mathbb{Z}_p[[\mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q})]] \cong \mathbb{Z}_p[[X]]$-module. The ring $\mathbb{Z}_p[[X]]$ is convenient since it is also the ring of special $p$-adically analytic functions consisting of power series with bounded coefficients. Assume that $M$ is finitely generated torsion as a $\mathbb{Z}_p[[X]]$-module. An *Iwasawa Main Conjecture* asks if the ideal generated in $\mathbb{Z}_p[[X]]$ by an analytic object, a $p$-adic $L$-function $L_p(X) \in \mathbb{Z}_p[[X]]$, is equal to the *characteristic ideal* (the $\mathbb{Z}_p[[X]]$-module theoretic analogue of *size*) of the algebraic object $M$:

$$\begin{array}{cc} \text{(analytic)} & \text{(algebraic)} \\ \mathbb{Z}_p[[X]] & \mathbb{Z}_p[[X]] \\ \cup & \cup \\ (L_p(X)) & \stackrel{?}{=} \mathrm{Char}_{\mathbb{Z}_p[[X]]}(M) \end{array}$$

## § 2.2. Iwasawa Theory for elliptic curves: The Ordinary Case

On the *analytic* side, Mazur and Swinnerton-Dyer defined in [MSD] a $p$-adic $L$-function so that we should have $L_p(E, X) \in \mathbb{Z}_p[[X]]$. Here, the ordinary assumption is needed to ensure that $L_p(E, X)$ has coefficients in $\mathbb{Z}_p$, i.e. $p$-adically bounded by 1. (If one follows their choice of normalization, or "period," we only know that $L_p(E, X) \in \mathbb{Q} \otimes \mathbb{Z}_p[[X]]$. This means we can find an integer $m$ so that all coefficients are in the $p$-adically bounded set $\mathbb{Z}_p \otimes \mathbb{Z}[\frac{1}{m}]$, and is not a major issue. We shall not discuss this point further, since one can always renormalize so that the bound is 1.) From the boundedness of the coefficients, we conclude that $L_p(E, X)$ has finitely many zeros.

On the *algebraic* side, we have the Selmer group which fits into an exact sequence (see e.g. [Sil]):

$$0 \to E(\mathbb{Q}_n) \otimes \mathbb{Q}/\mathbb{Z} \to \mathrm{Sel}(E/\mathbb{Q}_n) \to Ш(E/\mathbb{Q}_n) \to 0,$$

where $\mathbb{Q}_n$ denotes the $n$th layer in the cyclotomic $\mathbb{Z}_p$-extension $\mathbb{Q}_\infty$. It is really the $p$-primary part of this sequence that we consider. We now consider the limit of the duals of the $p$-primary Selmer groups:

$$\mathcal{X} := \varprojlim_n \mathrm{Hom}(\mathrm{Sel}_p(E/\mathbb{Q}_n), \mathbb{Q}_p/\mathbb{Z}_p).$$

This construction of $\mathcal{X}$ so far works whether $p$ is ordinary or not, but only in the ordinary case does $\mathcal{X}$ become a finitely generated torsion $\mathbb{Z}_p[[X]]$-module, by results of Rubin and Kato. Consequently, we can define $\mathrm{Char}_{\mathbb{Z}_p[[X]]}$ when $p$ is ordinary. Mazur's Main Conjecture asks whether $(L_p(E, X)) = \mathrm{Char}_{\mathbb{Z}_p[[X]]}\, \mathcal{X}$.

## § 2.3. Iwasawa Theory for elliptic curves: The Supersingular Case

On the *analytic* side, there are two $p$-adic $L$-functions $L_\alpha(E, X)$ and $L_\beta(E, X)$ ([AV75], [Vi76], [MTT]) for each choice of root $\alpha$ and $\beta$ of the Hecke polynomial $Y^2 -$

$a_pY+p$, which generalize that of Mazur and Swinnerton-Dyer. The problem is that they are not elements of $\mathbb{Z}_p[[X]]$, but of $\mathbb{Q}_p(\alpha)[[X]]$.[1] This causes $L_\alpha(E,X)$ and $L_\beta(E,X)$ to have infinitely many zeros.

The corresponding problem on the *algebraic* side is that $\mathcal{X}$ is not torsion as a $\mathbb{Z}_p[[X]]$-module.

These obstacles did not stop Perrin-Riou and Kato from formulating Main Conjectures in this setting! However, the objects involved are more complicated, and it had been more desirable to formulate an easier main conjecture, but it seemed for a long time that such an easier main conjecture didn't exist. The essential insight is about the number of main conjectures: The $\sharp/\flat$ philosophy sketched below gives rise to a *pair* of main conjectures.

In the case $a_p = 0$, Kobayashi constructed a pair of maps

$$\varprojlim_n H^1(\mathbb{Q}_{n,p},T) \xrightarrow{(\mathrm{Col}^\sharp,\mathrm{Col}^\flat)} \mathbb{Z}_p[[X]]^{\oplus 2},$$

in [Ko03], where $T$ is the Tate module and $\mathbb{Q}_{n,p}$ is the completion of $\mathbb{Q}_n$. For the general supersingular case, see [S12]. These maps are elliptic curve analogues of a classical map given by Coleman in [Co79], and send an Euler system, Kato's zeta element[2], to a pair of $p$-adic $L$-functions $\left(L_p^\sharp(E,X), L_p^\flat(E,X)\right) \in \mathbb{Z}_p[[X]]^{\oplus 2}$. When $a_p = 0$, this pair has been constructed by Pollack and by the author in the general case. It satisfies

$$(L_\alpha(E,X), L_\beta(E,X)) = \left(L_p^\sharp(E,X), L_p^\flat(E,X)\right) \mathcal{L}og_{a_p}, \text{where}$$

$$\mathcal{L}og_{a_p} := \lim_{n\to\infty} \begin{pmatrix} a_p & 1 \\ \Phi_p(1+X) & 0 \end{pmatrix} \begin{pmatrix} a_p & 1 \\ \Phi_{p^2}(1+X) & 0 \end{pmatrix} \cdots \begin{pmatrix} a_p & 1 \\ \Phi_{p^n}(1+X) & 0 \end{pmatrix} \begin{pmatrix} a_p & 1 \\ -p & 0 \end{pmatrix}^{-(n+2)} \begin{pmatrix} -1 & -1 \\ \beta & \alpha \end{pmatrix}.$$

We note that $\mathcal{L}og_{a_p}$ is a $2\times 2$ matrix whose entries are $p$-adic analytic functions converging on the open unit disk. Here, $\Phi_n$ denotes the $n$th cyclotomic polynomial. The matrix $\mathcal{L}og_{a_p}$ is responsible for the infinitely many zeros of $L_\alpha$ and $L_\beta$, but once we divide the vector $(L_\alpha, L_\beta)$ by $\mathcal{L}og_{a_p}$, a vector $(L_\sharp, L_\flat)$ with finitely many zeros appears. Intuitively, dividing the vector $(L_\alpha, L_\beta)$ by $\mathcal{L}og_{a_p}$ is like multiplying the Riemann zeta function $\zeta(s)$ by the Gamma function $\Gamma(s)$. The vector $(L_\alpha, L_\beta)$ has infinitely many uninteresting zeros, just like $\zeta(s)$ has infinitely many trivial zeros. $\Gamma(s)$ and $\mathcal{L}og_{a_p}$ factor out the non-interesting zeros, until only the interesting zeros remain.

The $\sharp/\flat$ theory is much easier when $a_p = 0$. For example, we can explicitly describe the entries of $\mathcal{L}og_{a_p}$, since all but one of the matrices involved in its definition are anti-diagonal.

---

[1] In fact, they can be considered as elements of a smaller subring $\mathcal{H}^{\frac{1}{2}}(X)$ consisting of analytic functions converging on the $p$-adic unit disk whose power series coefficients grow like $\log_p^{\frac{1}{2}}(1+X)$, where $\log_p(1+X)$ is the $p$-adic logarithm.

[2] or more exactly, its local image

The kernels of each of the maps $\mathrm{Col}^\sharp$ and $\mathrm{Col}^\flat$ give rise to new local conditions, producing a pair of Selmer group duals $\mathcal{X}^\sharp$ and $\mathcal{X}^\flat$ which are finitely generated torsion $\mathbb{Z}_p[[X]]$-modules. More precisely, $\mathcal{X}^{\sharp/\flat}$ is the Pontryagin dual of the $\sharp/\flat$-Selmer group. Recall that a Selmer group of a $\mathrm{Gal}_K$-representation $R$ of a number field $K$ is a kernel:

$$\mathrm{Sel}(K,R) = \ker\left(H^1 \to \prod_v H^1_v/S_v\right),$$

where $H^1$ is the *global* cohomology group $H^1(K,R)$ and $H^1_v$ its local counterpart[3] $H^1(K_v,R)$ for a place $v$ of $K$. For example, for the Selmer group $\mathrm{Sel}(E/\mathbb{Q}_n)$, we have $K=\mathbb{Q}_n$, $R=W$, where $V:=T\otimes\mathbb{Q}_p$, $W=V/T$, and $S_v = E(\mathbb{Q}_{n,v})\otimes\mathbb{Q}_p/\mathbb{Z}_p$.

When $p|a_p$, the local condition $S_p$ causes $\mathcal{X} = \mathrm{Hom}\left(\varprojlim_n \mathrm{Sel}(\mathbb{Q}_n,W), \mathbb{Q}_p/\mathbb{Z}_p\right)$, the Pontryagin dual, to be not $\mathbb{Z}_p[[X]]$-torsion. To define the Selmer group $\mathrm{Sel}^{\sharp/\flat}(\mathbb{Q}_\infty,W)$, we replace $S_p$ by finer submodules $S_p^{\sharp/\flat} \subset S_p \subset H^1(\mathbb{Q}_{\infty,p},W)$. The modules $S_p^{\sharp/\flat}$ are defined to be the exact annihilators of $\ker \mathrm{Col}^{\sharp/\flat}$ under the Tate pairing $H^1(\mathbb{Q}_{\infty,p},T)\times H^1(\mathbb{Q}_{\infty,p},W)\to\mathbb{Q}_p/\mathbb{Z}_p$. The resulting Pontryagin duals $\mathcal{X}^{\sharp/\flat}$ are then $\mathbb{Z}_p[[X]]$-torsion, and we can formulate a pair of main conjectures, equivalent to main conjectures of Kato [Ka05] and Perrin-Riou [PR]:

*Conjecture* 2.1 ([Ko03] for $a_p=0$, [S12] for $p|a_p$).

$$\left(L_p^\sharp(E,X)\right) = \mathrm{Char}_{\mathbb{Z}_p[[X]]}\,\mathcal{X}^\sharp, \text{ and } \left(L_p^\flat(E,X)\right) = \mathrm{Char}_{\mathbb{Z}_p[[X]]}\,\mathcal{X}^\flat.$$

A consequence of a theorem of Kato [Ka05, Theorem 12.5], proved via constructing an integral Euler system, is that

$$(L_p^\sharp(E,X)) \subset \mathrm{Char}_{\mathbb{Z}_p[[X]]}\,\mathcal{X}^\sharp \text{ and } (L_p^\flat(E,X)) \subset \mathrm{Char}_{\mathbb{Z}_p[[X]]}\,\mathcal{X}^\flat$$

(under the same hypotheses of the image of the residual Galois representation as in [Ka05, Theorem 12.5]).

### § 2.4. Sketch of strategy for proving the main conjecture

We now sketch the strategy for proving the main conjecture in the case of elliptic curves. This generalizes ideas of Wan in the case $a_p=0$. The main difficulty when $a_p\neq 0$ is that many of the $\sharp/\flat$-objects can not be handled separately. Note that we carry out this strategy in [S] in the case of elliptic curves, which is why in this paper the notation is for elliptic curves. However, the general strategy outlined here should be applicable to the general weight two modular forms case. The main missing ingredient at the moment is a $\sharp/\flat$-theory.

[3] which is required to be the unramified classes for almost all $v$

The most important idea is to formulate equivalent main conjectures - this can be achieved once we work over an auxiliary quadratic field $K$. One is a main conjecture involving four $\sharp/\flat$ objects, and another one is a main conjecture in terms of a Greenberg-type Selmer group and a Greenberg-type $p$-adic $L$-function. The Greenberg-type main conjecture is amenable to a $GU(3,1)$-Eisenstein series argument which Wan carried out to prove one inclusion. Assuming equivalence of main conjectures, this inclusion then implies an inclusion in each of the four $\sharp/\flat$-main conjectures. (This resulting inclusion is in the reverse direction of the one that appears in Kato's work, but Kato's work is over $\mathbb{Q}$. If we could generalize Kato's work to $K$, we would be done.) Ideally, this inclusion would then directly specialize to the $\sharp/\flat$ main conjectures over $\mathbb{Q}$, giving a converse to the results in the previous section. However, there is an issue when specializing down to $\mathbb{Q}$ (we have to take into account quadratic twists by $K$), but this issue can be overcome.

The most important technical ingredient in [S] is thus to prove the equivalence of the four $\sharp/\flat$ main conjectures and the (one) Greenberg-type main conjecture. To do this, we prove that both are equivalent to a pair of main conjectures phrased in terms of a pair of *integral Euler systems*. These Euler systems are integral versions of the Euler systems of Beilinson–Flach elements, constructed by Kings, Loeffler, and Zerbes.

Thus, there are three equivalent formulations of the main conjecture, which we now explain in the three following subsections, in the context of elliptic curves. Denote by $K$ an auxiliary imaginary quadratic field in which the prime $p$ splits as $\mathfrak{pq}$. Denote by $K_\infty$ the maximal $p$-unramified $\mathbb{Z}_p$-extension of $K$. This is a $\mathbb{Z}_p^2$-extension which can be realized as the compositum of the towers of ray class fields $K(\mathfrak{p}^n)$ and $K(\mathfrak{q}^n)$. As in the case for $\mathbb{Q}$, we can define an Iwasawa algebra with variables $X$ and $Y$ corresponding each to $\mathfrak{p}$ and $\mathfrak{q}$. Denote this Iwasawa algebra by $\Lambda_K := \mathbb{Z}_p[[X,Y]]$.

## § 2.5. The Greenberg-type main conjecture

On the analytic side, there is an element $L_p^{\forall 0} \in \Lambda_K \otimes \mathbb{Q}$. The precise definition won't be used, so we just record that it comes from a Rankin-Selberg convolution of the elliptic curve and a CM form constructed from characters associated to $K$. A bit more precisely, this function interpolates twists of the $L$-function of the automorphic representation $\pi_E$ associated to $E$ by Hecke characters. (It interpolates values of the form $L(K, \pi_E, \xi, \frac{\kappa}{2} - \frac{1}{2})$, where $\xi$ runs over Hecke characters of $\mathbb{A}_K^\times / K^\times$ of infinity type $(\frac{\kappa}{2}, \frac{-\kappa}{2})$ for $\kappa \geqslant 6$ associated to elements of $\operatorname{Spec} \Lambda_K$. The interested reader is referred to [W2], which discusses $L_p^{\forall 0}$.)

The corresponding algebraic object should be an object which is finitely generated torsion as a $\Lambda_K$-module. We can produce such an object by making the local condition at one of the primes, say $\mathfrak{q}$, as fine/strict as possible. In fact, this allows to loosen the condition at the other prime $\mathfrak{p}$ completely. Thus, let us consider the following "coarse

at $\mathfrak{p}$ but fine at $\mathfrak{q}$" Selmer group[4]. We put $\mathcal{T} := T \otimes \Lambda_K(\Psi^{-1})$. The character $\Psi$ is the character $\mathrm{Gal}(\overline{K}/K) \to \mathrm{Gal}(K_\infty/K) \to \Lambda_K^\times$, where $K_\infty$ is the $\mathbb{Z}_p^2$-extension of $K$. We also put $\mathcal{W} := \mathrm{Hom}_{\mathbb{Z}_p}(\Lambda_K, \mathbb{Q}_p/\mathbb{Z}_p) \otimes \mathcal{T}$.

**Definition 2.1.**

$$\mathrm{Sel}_{\forall 0}(K, \mathcal{W}) := \ker\left( H^1(K, \mathcal{W}) \to \prod_{v \nmid p} H^1(I_v, \mathcal{W}) \times H^1(K_\mathfrak{q}, \mathcal{W}) \right)$$

We then put $\mathcal{X}_{\forall 0} := \mathrm{Hom}(\mathrm{Sel}_{\forall 0}(K, \mathcal{W}), \mathbb{Q}_p/\mathbb{Z}_p)$. This is finitely generated torsion as a $\Lambda_K$-module, so that we can define its characteristic ideal $\mathrm{Char}(\mathcal{X}_{\forall 0})$.

The reason for tensoring with $\Lambda_K(\Psi^{-1})$ is that by Shapiro's lemma, $\mathrm{Sel}_{\forall 0}(K, \mathcal{W}) = \varinjlim_{K \subseteq K' \subseteq K_\infty} \mathrm{Sel}_{\forall 0}(K', W)$, cf. [SU12, Proposition 3.4 and Section 3.1.3]. (The Selmer groups $\mathrm{Sel}_{\forall 0}(K', W)$ are defined as above with $K'$ instead of $K$ and $T$ instead of $\mathcal{W}$.)

The main conjecture is full equality in the following theorem of Wan [W, Theorem 2.13]:

**Theorem 2.2.** *Let $E$ have square-free conductor $N$ that has at least one prime divisor $l|N$ not split in $K$, and suppose that $E[p]|_{G_K}$ is absolutely irreducible, where $p \nmid N$ is odd and satisfies $p \mid a_p$. Then as (fractional) ideals of $\Lambda_K \otimes \mathbb{Q}$, we have*

$$\mathrm{Char}(\mathcal{X}_{\forall 0}) \subseteq (L_p^{\forall 0}).$$

## § 2.6. The four ♯/♭-main conjectures

In [Ki13], BD Kim generalized Kobayashi's construction of plus/minus Coleman maps to the two-variable case, but still assumed $a_p = 0$. In [S], we generalize Kim's construction to the general supersingular case. Thus, we construct ♯/♭-Coleman maps.

$$\mathrm{Col}_v^{\sharp/\flat} : \varprojlim_{n,m} H^1(K_{v,n,m}, T) \to \Lambda_K^2,$$

where $v$ can be $\mathfrak{p}$ or $\mathfrak{q}$, and $K_{v,n,m}$ denotes the compositum of the $n$th layer in the cyclotomic tower of $K_v$ and the $m$th layer in its unramified tower. In the case $a_p = 0$, both Kobayashi and Kim construct these from pairings in Galois cohomology used in the work of Kurihara and Perrin-Riou (discussed in [Ku02, Section 3]). Their essential insight was that $H^1(K_{v,n,m}, T)$ is generated by elements $c_{n,m}$ which could be appropriately modified to construct trace-compatible elements $c_{n,m}^{\pm}$. By pairing with $c_{n,m}^{+}$

[4] or "relaxed at $\mathfrak{p}$ but restricted/strict at $\mathfrak{q}$." We are following Coates's treminology [CS05] for the word "fine." The symbol $\forall$ stands for "coarse" because of the absence of restrictions, while the symbol 0 stands for "fine."

instead of $c_{n,m}$, they were able to construct a map $\mathrm{Col}_v^+$ which has bounded image, i.e. is in $\Lambda_K$, and similarly they constructed a map $\mathrm{Col}_v^-$ by working with $c_{n,m}^-$. Note that the constructions of $\mathrm{Col}_v^+$ and $\mathrm{Col}_v^-$ were *separate*. In the general supersingular case, these constructions break down, but the new insight in our works [S12, S] was the idea to turn the *failure* of trace-compatibility of $c_{n,m}$ into a *simultaneous* construction of $\mathrm{Col}_v^\sharp, \mathrm{Col}_v^\flat$ that generalizes the constructions of Kobayashi and Kim. The kernels of the $\sharp/\flat$-Coleman maps at the primes $\mathfrak{p}$ and $\mathfrak{q}$ give rise to the appropriate local conditions for modified Selmer groups $\mathrm{Sel}_{\sharp\sharp}$, $\mathrm{Sel}_{\sharp\flat}$, $\mathrm{Sel}_{\flat\sharp}$, and $\mathrm{Sel}_{\flat\flat}$ (giving rise to duals $\mathcal{X}_{\sharp\sharp}$, $\mathcal{X}_{\sharp\flat}$ etc. which are $\Lambda_K$-torsion, cf. [S, Proposition 2.23]). More precisely, here is the definition for $\mathrm{Sel}_{\sharp\flat}$:

$$\mathrm{Sel}_{\sharp\flat} := \ker\left(\mathrm{Sel}(E/K_\infty) \to \frac{\varinjlim_m \varinjlim_n H^1(K_{\mathfrak{p},n,m}, W)}{E^\sharp} \times \frac{\varinjlim_m \varinjlim_n H^1(K_{\mathfrak{q},n,m}, W)}{E^\flat}\right)$$

Here, the subindices each describe local conditions at the prime $\mathfrak{p}$ resp. the prime $\mathfrak{q}$, so that the local conditions are the exact annihilator $E^\sharp$ under the Tate pairing as before of $\ker \mathrm{Col}_\sharp$ at the prime $\mathfrak{p}$, and $E^\flat$ is the exact annihilator of that of $\ker \mathrm{Col}_\flat$ at the prime $\mathfrak{q}$.

Fortunately, the analytic counterparts to these objects already exist - they are the four signed $p$-adic $L$-functions $L_{\sharp\sharp}, L_{\sharp\flat}, L_{\flat\sharp}, L_{\flat\flat}$ due to Antonio Lei [Lei12]. These $p$-adic $L$-functions interpolate special values of the Hasse-Weil $L$-function twisted by appropriate characters $\chi$ of the group $\mathrm{Gal}(K_\infty/K)$. One challenge is to prove that they live in $\Lambda_K$ rather than $\Lambda_K \otimes \mathbb{Q}$. The $\sharp/\flat$ main conjectures then are four (equivalent[5]) statements of the following form :

*Conjecture* 2.2. Let $\circ, * \in \{\sharp, \flat\}$. Then

$$(L_{\circ *}) = \mathrm{Char}(\mathcal{X}_{\circ *})$$

Note that we have four possibilities to choose $\circ$ and $*$, which is the reason why we have four main conjectures.

## § 2.7. The pair of main conjectures using integral Euler systems

The Beilinson-Flach elements $\Delta_\alpha$ and $\Delta_\beta$ constructed in [KLZ] by Kings, Loeffler, and Zerbes are Euler systems which incarnate Rankin-Selberg convolutions of modular forms. Under an appropriate exponential map, one can recover the special values of the Hasse-Weil $L$-function at 1, twisted by characters of $\mathrm{Gal}(K_\infty/K)$. Their natural habitat is a (Galois) cohomology group $H^1(K, \mathcal{T}) \otimes_{\Lambda_K} \mathcal{H}_K(\mathrm{Gal}(K_\infty/K))$.

$H^1(K, \mathcal{T})$ is a rank two $\Lambda_K$-module (see e.g. [S, Proof of Proposition 2.42]), while $\mathcal{H}_K(\mathrm{Gal}(K_\infty/K))$ is the distribution algebra on $\mathrm{Gal}(K_\infty/K)$ with coefficients in $K$.

[5] they are equivalent to each other when the $p$-adic $L$-functions are not zero

($\mathcal{H}_K(\mathrm{Gal}(K_\infty/K))$ can be replaced by a subring with more precise growth conditions.) There is a map $\log_{\mathfrak{p}}$ (the Bloch-Kato logarithm) that connects $\Delta_{\alpha/\beta}$ and $L_p^{\forall 0}$. A bit more precisely, we can say that for $\xi = \alpha$ or $= \beta$, "$\log_{\mathfrak{p}}(\Delta_\xi)$ at $\varphi$" = "$L_p^{\forall 0} \times \xi^{-\mathfrak{f}_\varphi}$ at $\varphi$," where $\varphi$ corresponds to a character of the Galois group of a finite extension of $\mathcal{K}_{\mathfrak{p}}$ and $\mathfrak{f}_\varphi$ is its conductor. (For the precise statement of the above sentence in quotation marks, see [W, Proposition 7.6] and [KLZ, Theorems 7.1.4/5].)

However, what we desire is a map that sends an Euler system to the $p$-adic $L$-function directly, rather than a collection of special values. To accomplish this, we construct *integral* Euler systems (explained below) and a pair of integral versions of $\log_{\mathfrak{p}}$, the Wan maps explained in the next subsection. For the integral Euler system, one can factor the matrix $\mathcal{L}og_{a_p}$ out of the pair of Euler systems of Kings, Loeffler, and Zerbes, in analogy to the case of $p$-adic $L$-functions:

**Theorem 2.3** ([S], generalizing [W] which assumes $a_p = 0$)**.** *There are elements $\Delta_\sharp$ and $\Delta_\flat$ which are in $H^1(K, \mathcal{T})$ so that we have*

$$h \times (\Delta_\alpha, \Delta_\beta) = (\Delta_\sharp, \Delta_\flat)\mathcal{L}og_{a_p}$$

(The matrix $\mathcal{L}og_{a_p}$ is formally the same as before, but the meaning of the variable $X$ is different - in subsection 2.3, it corresponded to $p$, while here it correponds to $\mathfrak{p}$. The constant $h$ is an element of $\Lambda_K$.)

To formulate the main conjecture, we then need to define Selmer groups $\mathrm{Sel}_{\hat{\sharp}\forall}$ (resp. $\mathrm{Sel}_{\hat{\flat}\forall}$). Here is the definition:

$$\mathrm{Sel}_{\hat{\sharp}\forall} := \ker\left(H^1(K,\mathcal{T}) \to \prod_{v\nmid p} H^1(I_v,\mathcal{T}) \times \frac{H^1(K_{\mathfrak{p}},\mathcal{T})}{\ker \mathrm{Col}_{\mathfrak{p}}^{\sharp}}\right)$$

To prepare for the relation with the Greenberg-type main conjecture, we must also define a Selmer group $\mathcal{X}_{\sharp 0}$ (resp. $\mathcal{X}_{\flat 0}$) whose local condition is empty everywhere except at the prime $\mathfrak{p}$, where it is the dual of $\ker \mathrm{Col}_\sharp$ (resp. $\ker \mathrm{Col}_\flat$). The Greenberg-type Selmer group has as its local conditions the empty condition everywhere except at $\mathfrak{p}$, where the local conditions is everything. Thus, our $\mathcal{X}_{\sharp 0}$ is just the Greenberg-type Selmer group with the local condition modified at $\mathfrak{p}$, just like Kobayashi's Selmer groups were the usual Selmer groups with the local conditions modified at $p$:

$$\mathrm{Sel}_{\sharp 0} := \ker\left(H^1(K,\mathcal{W}) \to \prod_{v\nmid p} H^1(I_v,\mathcal{W}) \times \frac{H^1(K_{\mathfrak{p}},\mathcal{W})}{E^{\sharp}} \times H^1(K_{\mathfrak{q}},\mathcal{W})\right)$$

Recall that $\mathcal{W} = \mathrm{Hom}_{\mathbb{Z}_p}(\Lambda_K, \mathbb{Q}_p/\mathbb{Z}_p) \otimes \mathcal{T}$.

We define $\mathcal{X}_{\sharp 0} := \mathrm{Hom}(\mathrm{Sel}_{\sharp 0}, \mathbb{Q}_p/\mathbb{Z}_p)$. Using a control theorem, the torsionness of $\mathcal{X}_{\sharp\sharp}$ implies that $\mathcal{X}_{\sharp 0}$ is torsion. To formulate a main conjecture, recall that we constructed $\Delta_{\sharp/\flat}$ so that they are elements of $H^1(K, \mathcal{T})$. It turns out that $\Delta_\sharp$ is in the rank one $\Lambda_K$-submodule $\mathrm{Sel}_{\hat{\sharp}\forall}$ of $H^1(K, \mathcal{W})$. The quotient $\Lambda_K$-module $\mathrm{Sel}_{\hat{\sharp}\forall}/\Delta_\sharp$ is torsion. We formulate the following main conjecture:

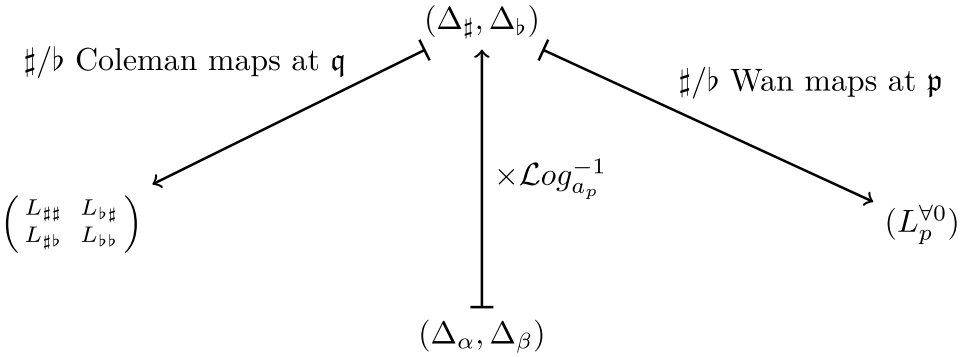
*Conjecture* 2.3.

$$\mathrm{Char}(\mathrm{Sel}_{\hat{\sharp}\forall}/\Delta_\sharp) = \mathrm{Char}(\mathcal{X}_{\sharp 0})$$

The corresponding discussion also holds for $\flat$-objects, so that there is a corresponding conjecture for the $\flat$-objects.

## § 2.8. Equivalence of the main conjectures

The main idea to prove equivalence of the three types of main conjectures is to connect the analytic objects to each other by the $\sharp$- and $\flat$- Coleman maps, and by $\sharp$- and $\flat$- Wan maps $\mathrm{Wan}_{\sharp/\flat} : H^1(K_\mathfrak{p}, \mathcal{W}) \to \Lambda_K \otimes \mathbb{Q}$. They can be constructed by an explicit description of $\ker \mathrm{Col}_{\sharp/\flat}$, resp. are an integral version of the map $\log_\mathfrak{p}$ described before.




In the above diagram, the Euler systems are sent to $p$-adic $L$-functions: We have $\mathrm{Col}_\sharp((\Delta_\flat)_\mathfrak{q}) = L_{\sharp\flat}$, and $\mathrm{Wan}_\sharp((\Delta_\sharp)_\mathfrak{p}) = \mathrm{Wan}_\flat((\Delta_\flat)_\mathfrak{p}) = L_p^{\forall 0}$, where $\Delta_v$ means $\Delta$ restricted to $v$.

To prove equivalence of the main conjectures, we use four-term sequence arguments first found in Kurihara [Ku02]: For example, proving the equivalence between the $\sharp\flat$ main conjecture and the $\sharp$ Beilinson–Flach element main conjecture can be accomplished by the sequence

$$0 \to \mathrm{Sel}_{\hat{\sharp}\forall}/\Delta_\sharp \to \Lambda_K/(L_{\sharp\flat}) \to \mathcal{X}_{\sharp\flat} \to \mathcal{X}_{\sharp 0} \to 0$$

obtained via the Poitou-Tate exact sequence. The exactness of characteristic ideals then gives equivalence of the statement

$$\mathrm{Char}(\Lambda_K/(L_{\sharp\flat})) = (L_{\sharp\flat}) = \mathrm{Char}(\mathcal{X}_{\sharp\flat})$$

and the statement

$$\mathrm{Char}(\mathrm{Sel}_{\hat{\sharp}\forall}/\Delta_\sharp) = \mathrm{Char}(\mathcal{X}_{\sharp 0}).$$

## References


[AV75] Amice Y., Vélu J., Distributions $p$-adiques associées aux séries de Hecke in Journées Arithmétiques de Bordeaux (Bordeaux, 1974), *Astérisque* **24-25**, Société Mathématique de France, Montrogue, 1975, 119–131.

[CS05] Coates J. , Sujatha R. , Fine Selmer groups of elliptic curves over $p$-adic Lie extensions, *Math. Ann.* **331** (2005), no. 4, 809 − 839.

[Co79] Coleman, R., Division values in local fields, *Inventiones Mathematicae*, **53** (1979), no. 2, 91–116.

[Ka05] Kato, K., $p$-adic Hodge theory and values of zera functions of modular orms, *Astérisque*, **295** (2004), 117–290.

[Ki13] Kim, BD, Signed Selmer groups in $\mathbb{Z}_p^2$-extensions, *Canadian Mathematical Bulletin*, July 2013.

[KLZ] Kings, G., Loeffler, D. , Zerbes, S. , Beilinson-Flach elements in Coleman families, submitted.

[Ko03] Kobayashi, S., Iwasawa theory for elliptic curves at supersingular primes, *Inventiones Mathematicae* **152** (2003), no.1, 1–36.

[Ku02] Kurihara, M. , On the Tate Shafarevich groups over cyclotomic fields of an elliptic curve with supersingular reduction I, *Inventiones Mathematicae* **149** (2002), 195–224.

[Lei12] Lei, A., Factorisation of two-variable $p$-adic $L$-functions, *Canadian Mathematical Bulletin*, **57(4)**, 2014, 845-852.

[MSD] Mazur, B., Swinnerton-Dyer, P., Arithmetic of Weil curves, *Inventiones Mathematicae* **25** (1974), 1–61.

[MTT] Mazur, B. , Tate, J. , and Teitelbaum, J. , On p-adic analogues of the conjectures of Birch and Swinnerton-Dyer, *Inventiones Mathematicae* **84** (1986), 1–48.

[PR] Perrin-Riou, B. Fonctions $L$ $p$-adiques des représentations $p$-adiques, *Astérisque*, **229** (1995), 198 pp.

[PR04] Pollack, R. , Rubin, K. , The main conjecture for CM elliptic curves at supersingular primes, *Annals of Mathematics*, **159**(2004), no.1, 447 -464 .

[Ru91] Rubin, K. , The “main conjectures" of Iwasawa theory for imaginary quadratic fields, *Invent. Math.* **103** (1991), 25–68.

[Sil] Silverman, J., *The Arithmetic of Elliptic Curves*, Second Edition, Graduate Texts in Mathematics **106** (2009), Springer, New York.

[SU12] Skinner, C. , Urban, E. , The Main Conjectures for $GL(2)$, *Inventiones Mathematicae* **195** (2014), no. 1, 1–277.

[S12] Sprung, F. , Iwasawa theory for elliptic curves at supersingular primes: A pair of Main Conjectures, *Journal of Number Theory* **132** (2012), no. 7.

[S] Sprung, F. , The Iwasawa Main Conjecture for elliptic curves at odd supersingular primes, submitted, *http://arxiv.org/abs/1610.10017*

[W] Wan, X. Iwasawa Main Conjecture for Supersingular Elliptic Curves, submitted , *http://arxiv.org/abs/1411.6352*

[W2] Wan, X. Iwasawa Main Conjecture for Rankin-Selberg $p$-adic $L$-functions: Non-Ordinary Case, submitted

[Vi76] Vishik, M. Nonarchimedean measures associated with Dirichlet series, *Matematičeskii Sbornik* **99 (141)**, no. 2 (1976), pp. 248-260, 296.